RSAC 2025 Conference

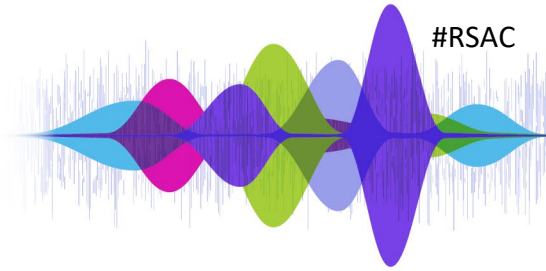
Many Voices.
One Community.

SESSION ID: APP-T01

The Next Twenty Years: What AppSec Needs to Do to Cement the Future

Christopher Romeo

CEO
Devici
https://www.linkedin.com/in/securityjourney/



Disclaimer

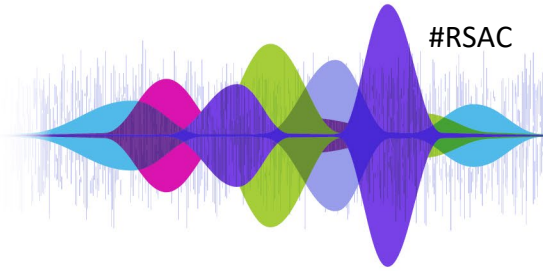
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

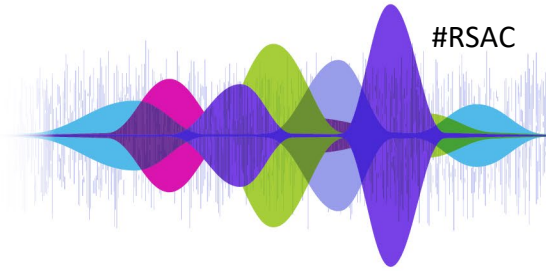
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

© 2025 Devici, Inc. or its affiliates. The Devici logos and other trademarks are proprietary. All rights reserved.

Agenda



- The current state of AppSec
- An AppSec postmortem
- A {scary?} future for AppSec
- The next three years



AppSec is dead, or is this the golden age of AppSec?

OWASP SINCE THE DAWN OF TIME (2003)

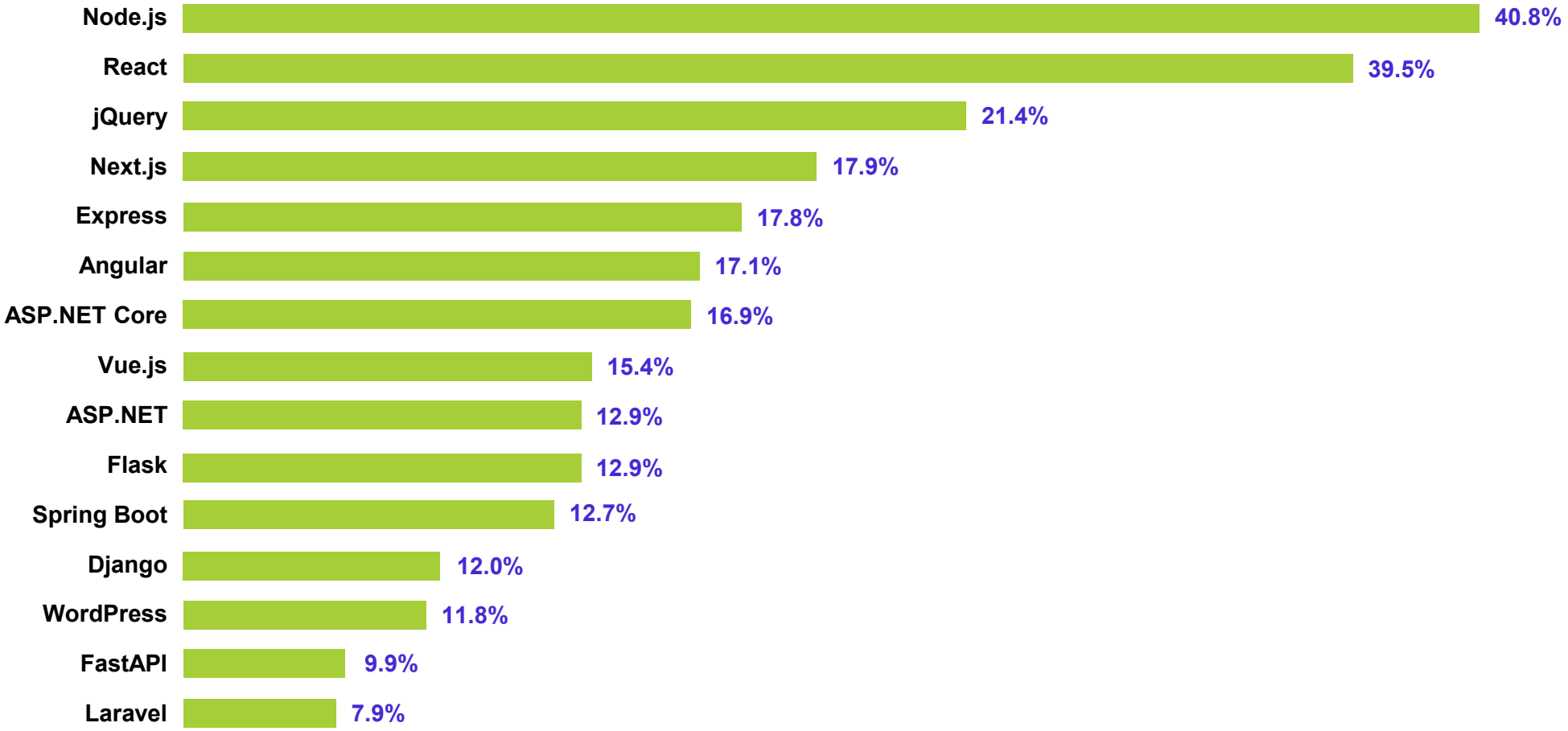
The language

1	Python	18.04%
2	C++	10.04%
3	C	9.17%
4	Java	9.16%
5	C#	6.39%
6	JavaScript	3.91%
7	SQL	2.21%
8	Visual Basic	2.18%
9	Go	2.03%
10	Fortran	1.79%

11	MATLAB	1.72%
12	Delphi/Object Pascal	1.63%
13	PHP	1.46%
14	Rust	1.28%
15	Ruby	1.28%
16	Swift	1.28%
17	Assembly Language	1.21%
18	Kotlin	1.13%
19	R	1.11%
20	Scratch	1.09%

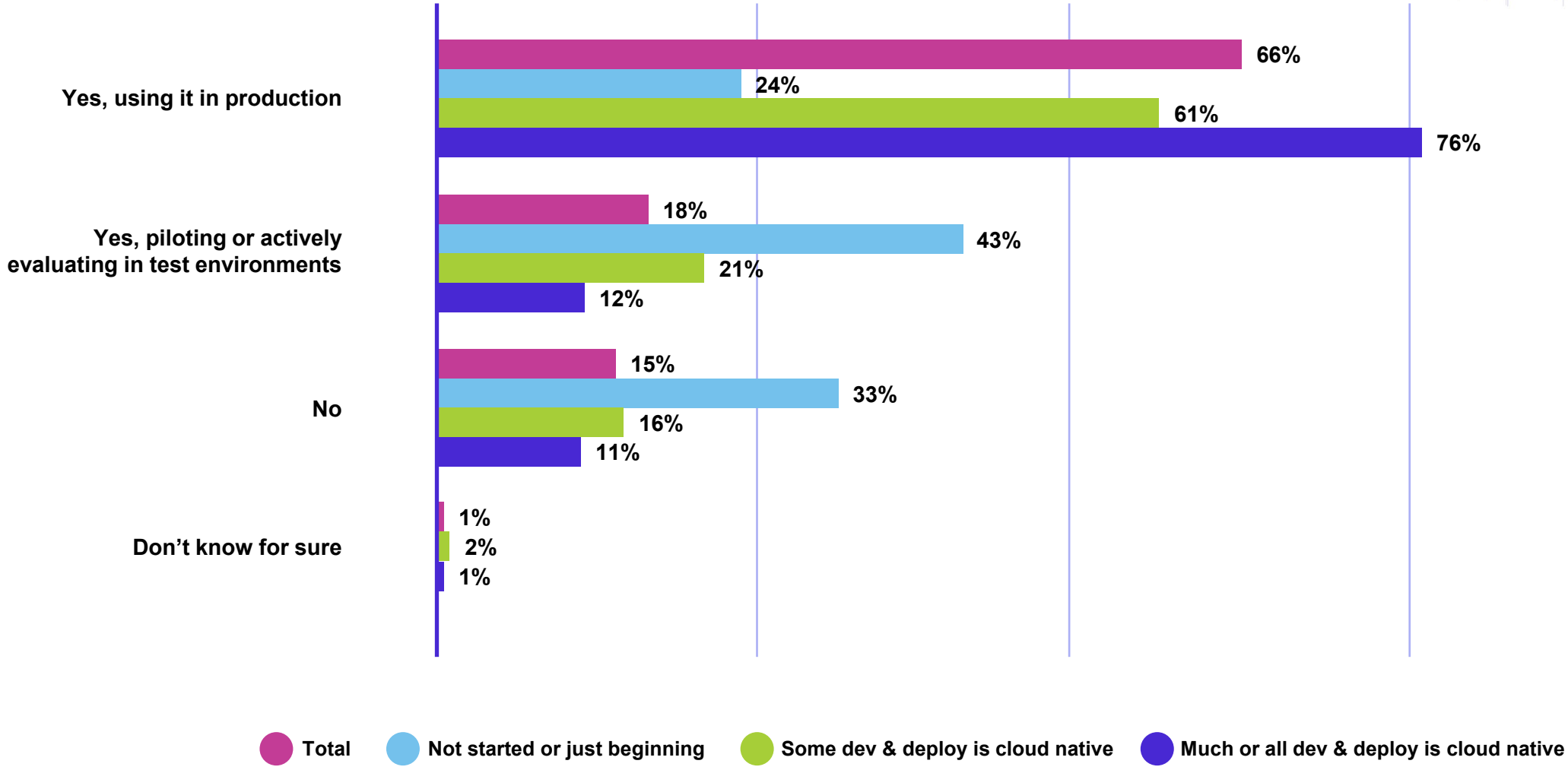
Source: https://www.tiobe.com/tiobe-index/, September 2024 data

Top web frameworks by usage



Source: https://www.statista.com/statistics/1124699/worldwide-developer-survey-most-used-frameworks-web

Cloud native adoption

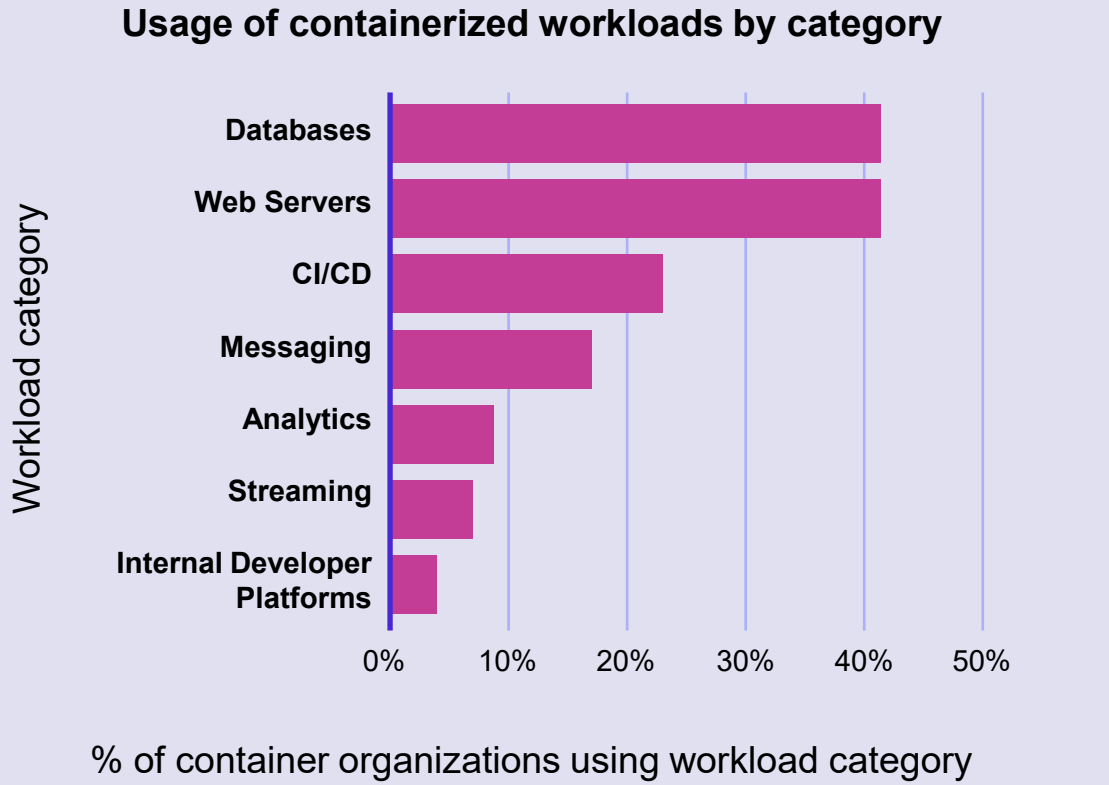


Source: https://www.cncf.io/reports/cncf-annual-survey-2023

Containerization

Databases and web servers are the leading workload categories for containers

Source: Datadog



Cloud complexity

23%
Have more than 100 cloud accounts

90%
Use multiple cloud providers

Source: https://www.firefly.ai/state-of-iac-report-2024, https://explodingtopics.com/blog/cloud-computing-stats

Agile and DevOps are normal

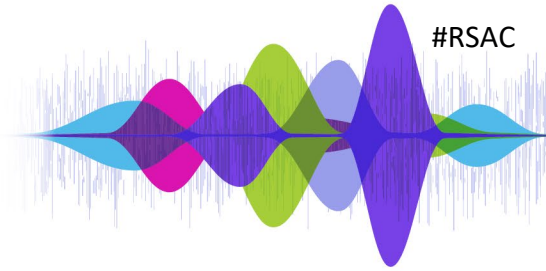
83%

report using DevOps practices within their organizations.

71%

report using Agile practices.

Source: https://www.strongdm.com/blog/devops-statistics



Application summary

A plethora of languages, with new languages introduced yearly.

Diversification of web frameworks.

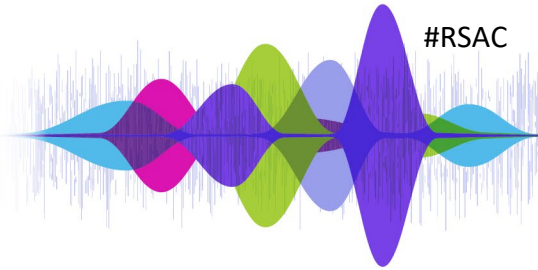
Cloud native is the new normal.

Everything runs in a container.

Cloud complexity across multiple providers.

Agile and DevOps are everywhere.

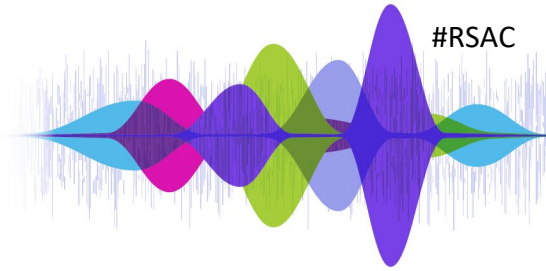
The state of AppSec



1. Issue density vs. tool fidelity.
2. The hamster wheel of scan and fix or a lack of secure by design/default.
3. Reachability and exploitability of vulnerabilities.
4. Lack of connection with operations.
5. Threat and risk expansion:
   - OWASP Top Ten (Web App 2021{5}, API 2023, CI/CD, LLM))

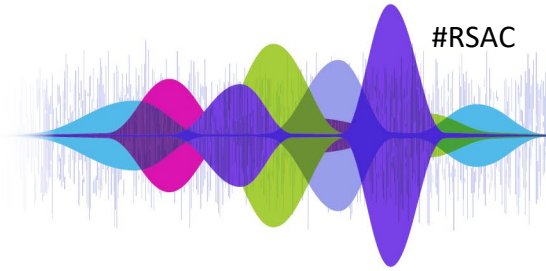
RSAC 2025 Conference

The AppSec Postmortem



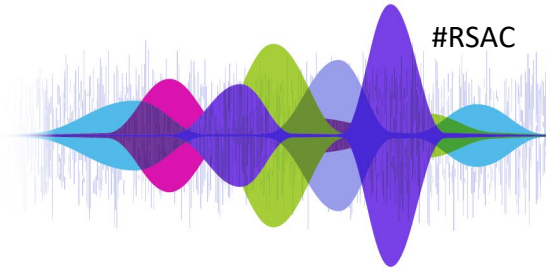
#1

Lack of a badge.

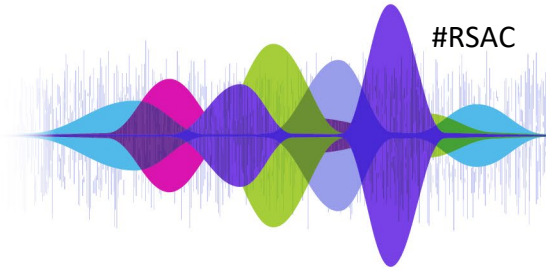


#2

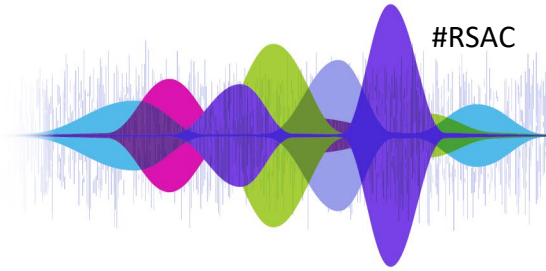
Overhyped.



Missed the window?

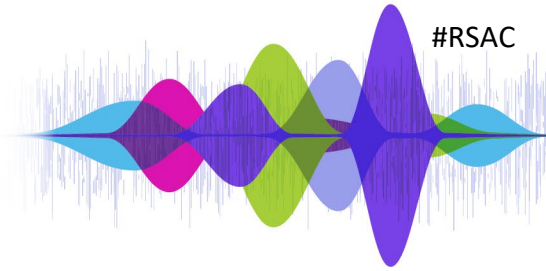


Education takes ten years to pay off.



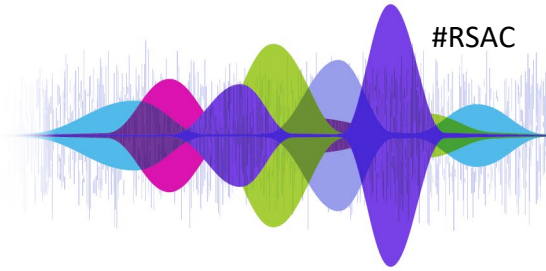
#5

Over-reliance on red.

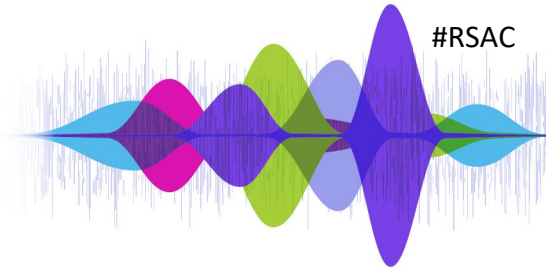


#6

OWASP and Commercialization.

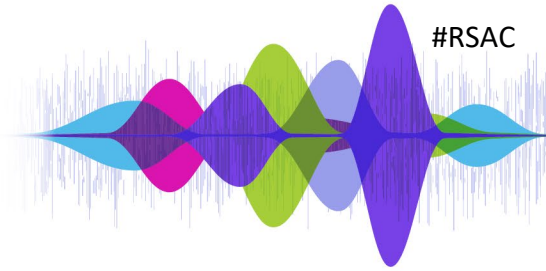


Provenance or lack thereof.



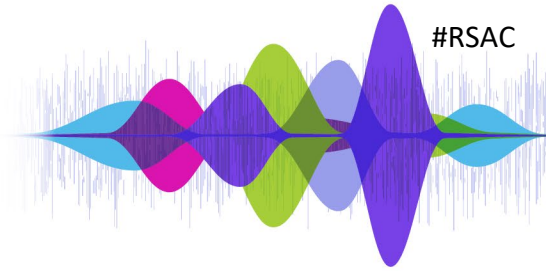
#8

Government lag.



#9

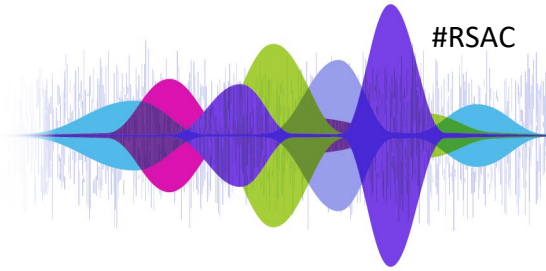
Good enough.



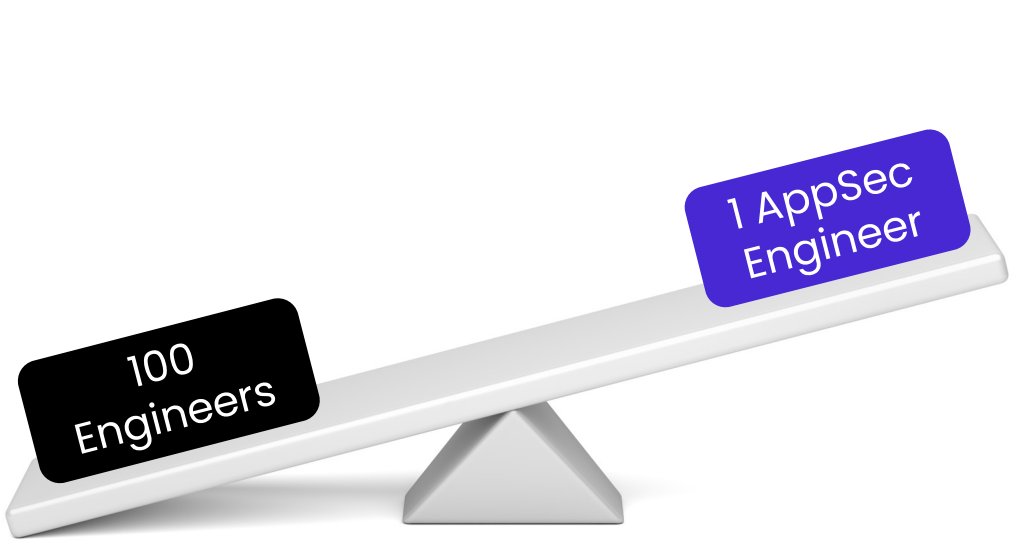
Driving slowly in the fast lane.

RSAC™ 2025 Conference

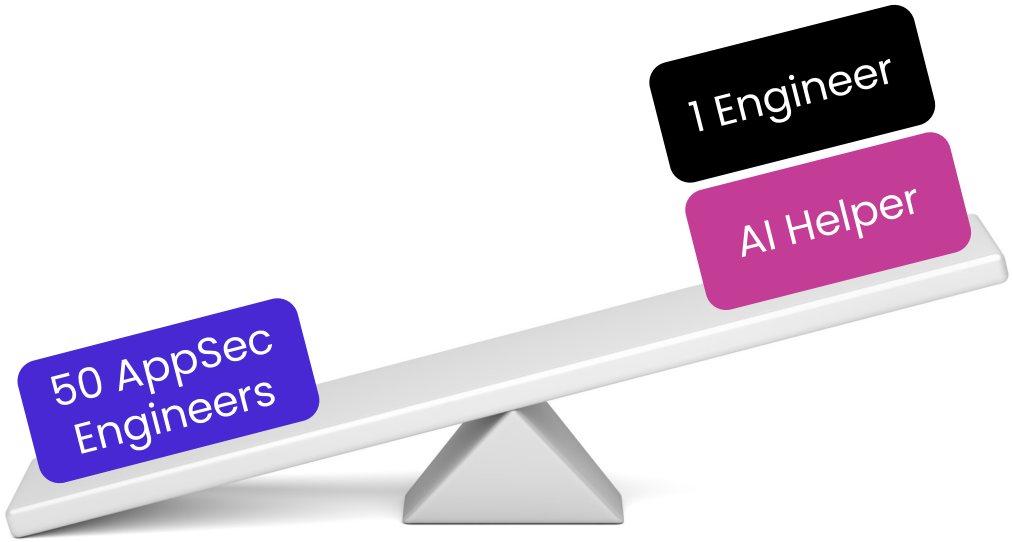
A brighter AppSec future (or what you can expect from the future)



Reducing complexity is the primary motivator of the AppSec future.

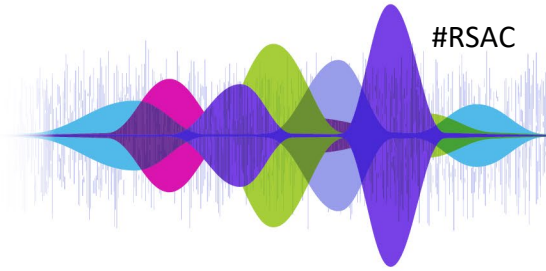


Today



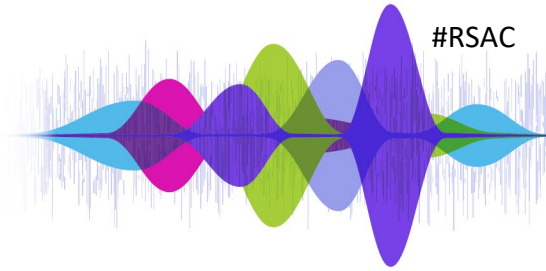
Future

Source: Kyle Kelly, https://www.linkedin.com/in/kylek42



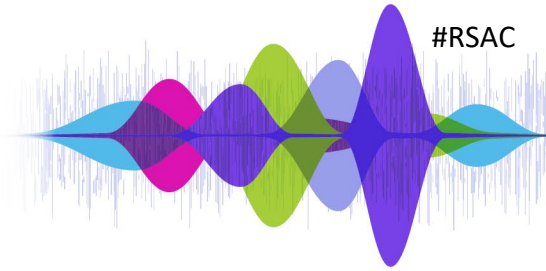
#1

AppSec is engulfed by Engineering. Engineer includes {software, AppSec}.



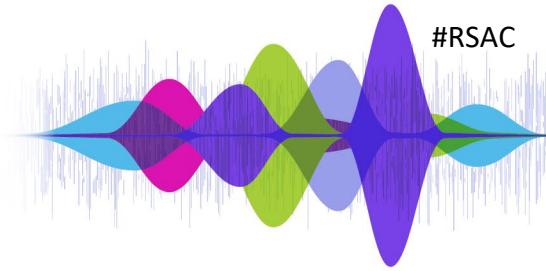
#2

Languages and frameworks built on robust security and privacy will thrive, while outdated ones fade into obscurity.



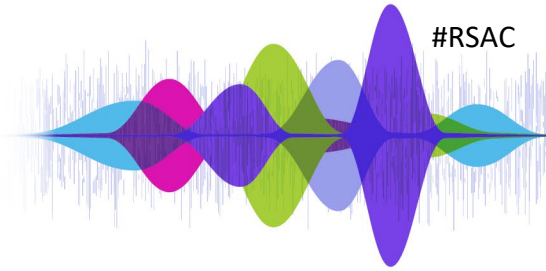
#3

A true “shift” from security tooling identifying problems to fixing problems and the death of legacy tools (SAST, DAST, SCA, WAF, etc.)



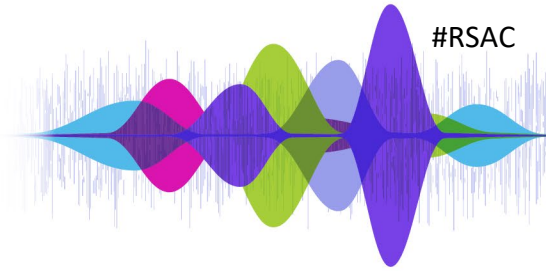
#4

The robots will rise, and AI agents will write software and design hardware entirely.



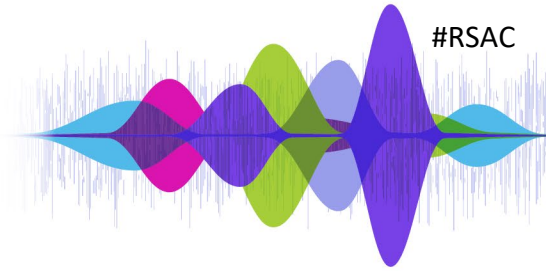
#5

The cloud will be ubiquitous and completely abstract, and the AI agents will interact directly.



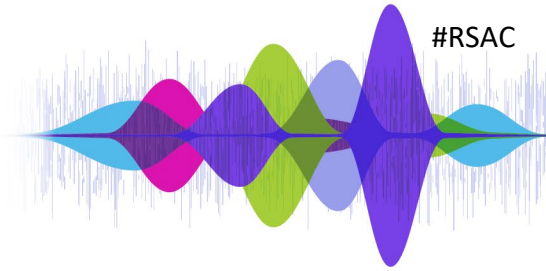
#6

Great trust will be placed in things that Engineering doesn’t understand.



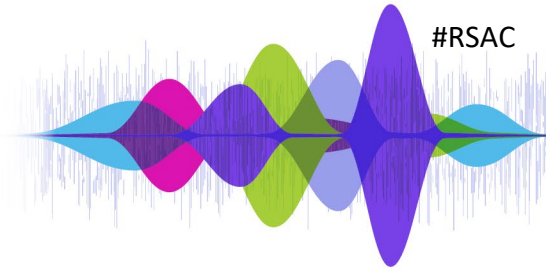
#7

Security becomes compliance only and focuses on inspections.



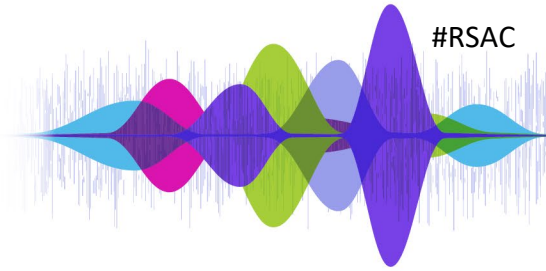
#8

Legally tested liability and warranty coverage for software and hardware purchasers becomes the standard.



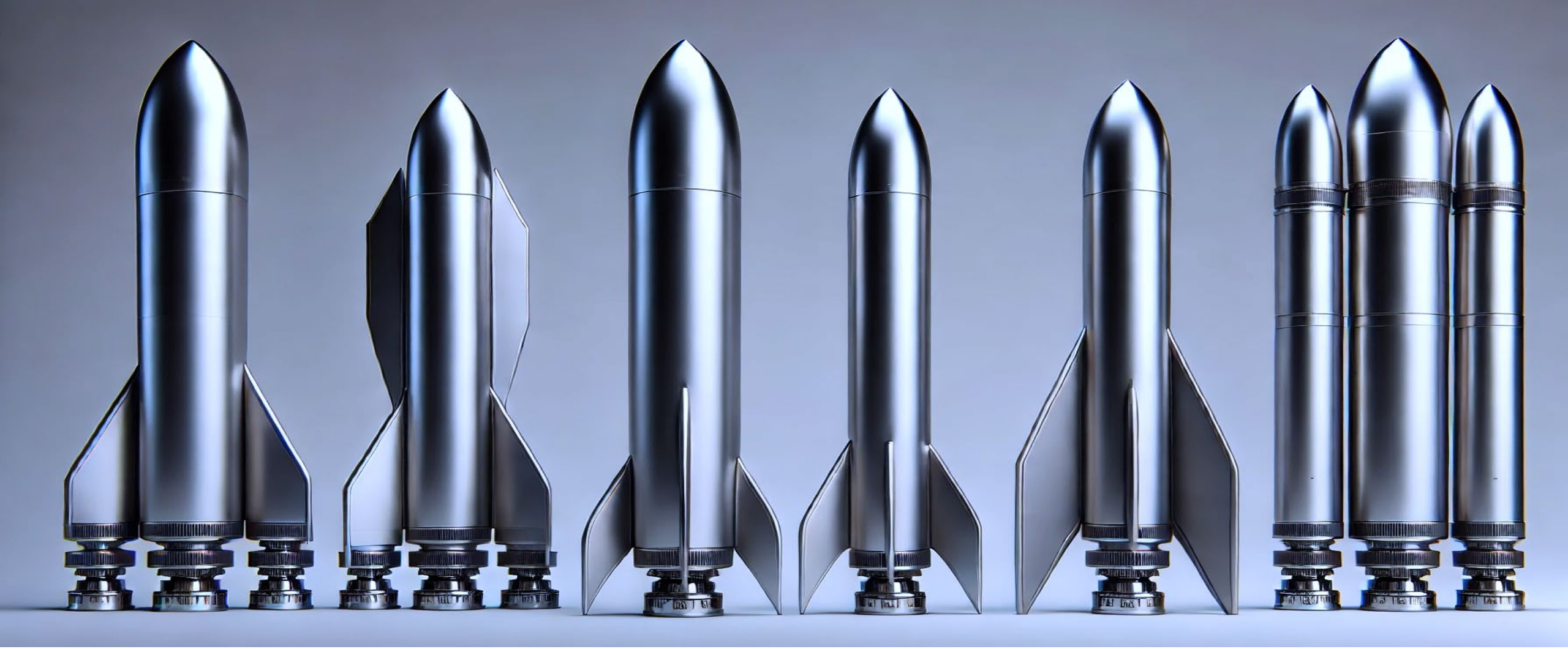
#9

Engineers graduate from the university system with a solid foundation of security and privacy.

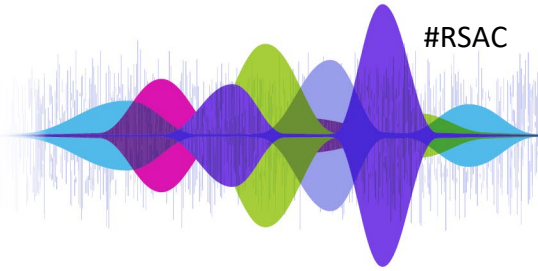


#10

Governments worldwide impose strict regulations and oversight on the development of software and hardware using AI.



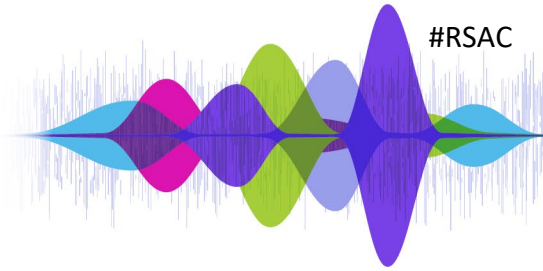
Are you scared yet?



What can we do to protect the future?

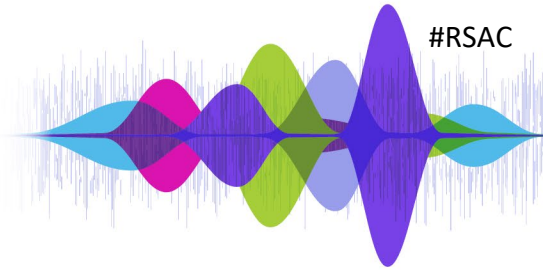
- Solving the trust problem with AI is crucial.
- Industry partnerships with the government must be made for realistic security and privacy controls.
- The Three Laws of Robotics (Asimov, 1942) must be the foundation for the AI takeover of Engineering.
  - “A robot may not injure a human being or, through inaction, allow a human being to come to harm.”
  - “A robot must obey the orders given it by human beings, except where such orders would conflict with the First Law.”
  - “A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.”
- We must introduce a layer of transparent observability outside the control of the AI.

The next one to three years



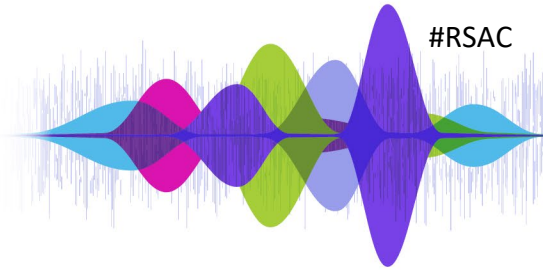
- Build a stronger alliance with your engineering team and proactively prepare to integrate with them as a seamless part of their processes.
- Move beyond dismissing AI as hype; invest in understanding its foundations, mechanics, and practical uses.
- Continuously evaluate emerging AI-powered security tools, positioning your program to adopt them effectively at the right time.
- Continue investing in your current legacy technologies until 2027 while formulating and executing an organized decommissioning strategy.
- Acknowledge that AppSec is in its ‘golden age’ today but anticipate significant changes within the next three years.

Apply what you have learned



- **Month 1:**
  - Ponder where your AppSec role or program fits against the post- mortem. Are you better off or worse?
- **Month 2:**
  - Think deeply about how AI will impact your future and how you can get involved now to help solve the trust and Government challenges.
- **Month 3:**
  - Take a vacation, because the AI overlords may have already taken over the writing of code and security functions.

Key takeaways



- Modern applications are complex and have many moving parts, complicating security and privacy.
- Application security has some issues.
- The postmortem highlighted challenges to AppSec from the past, but all can be overcome.
- The future is AI, and we can shape the future, but that train is already leaving the station, so get onboard.

devici

Questions?

Chris Romeo
CEO | Devici

chris@devici.com

Listen:
The Application Security Podcast
The Security Table
The Threat Modeling Podcast

RSAC™ 2025 Conference

Many Voices.
One Community.

Please visit https://devici.com/resources/blog